



Projeto de

**Regulamento Municipal da Política Geral de Segurança da
Informação do Município de Lagoa**

Publicado em Diário da República, ... Serie, Nº

Aviso .../..., de ... de ... de....

Nota Justificativa

A evolução da sociedade nas últimas décadas tem sido marcada, de forma intensa, pela acelerada digitalização das suas múltiplas áreas e domínios de atividade, sendo o ciberespaço apenas uma das facetas mais visíveis dessa mesma realidade.

O caráter extremamente dinâmico e fluido do ciberespaço, bem como a sua permanente mutação, coloca dificuldades permanentes, exigindo tais desafios respostas e medidas cada vez mais estruturadas por parte de múltiplas entidades.

Neste sentido, foi aprovada a Lei n.º 46/2018, de 13 de agosto, que consagrou o regime jurídico da segurança do ciberespaço e transpôs para o ordenamento jurídico nacional a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União. Mais recentemente foi aprovado o Decreto – Lei n.º 65/2021, de 30 de julho, que veio regulamentar a referida lei, estabelecendo requisitos que constituem um mínimo a assegurar pelas entidades abrangidas pelo mesmo diploma, contando-se entre os mesmos os requisitos de segurança das redes e sistemas de informação e, por outro lado, as regras para a notificação de incidentes, que devem ser cumpridos pela Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais.

Dando execução a tal regime jurídico, compete ao Município de Lagoa, no âmbito das suas competências e atribuições, garantir a segurança da informação, assegurando os níveis adequados de integridade, autenticidade, disponibilidade e confidencialidade, requeridos para a sua proteção, mitigando assim o impacto de eventuais incidentes que possam comprometer o regular funcionamento dos serviços municipais.

Neste enquadramento, torna-se absolutamente necessário a criação e aprovação do Regulamento Municipal da Política Geral de Segurança da Informação do Município de Lagoa, obedecendo às normas do quadro normativo em vigor.

**REGULAMENTO MUNICIPAL DA POLÍTICA GERAL DE SEGURANÇA
DA INFORMAÇÃO DO MUNICÍPIO DE LAGOA**

Artigo 1.º

Normas Habilitantes

O presente regulamento municipal é elaborado e aprovado ao abrigo da legitimação conferida pelo disposto nos artigos 112.º, n.º 7, *in fine* e 241.º, ambos da Constituição da República Portuguesa, na sua redação atual, nos artigos 135.º e seguintes do Código do Procedimento Administrativo, na sua redação atual, nos artigos 25.º, n.º 1, alínea g) e 33.º, n.º 1, alíneas k), ambos do anexo I à Lei n.º 75/2013, de 12 de setembro, na sua redação atual e nos artigos 2.º, n.º 1 e 7.º, n.º 1, al. a), ambos do Decreto – Lei n.º 65/2021, de 30 de julho.

Artigo 2.º

Objeto

Através do presente regulamento municipal são aprovadas as regras e normas em que assenta a Política Geral de Segurança da Informação do Município de Lagoa, visando dar cumprimento às obrigações previstas no Decreto – Lei n.º 65/2021, de 30 de julho.

Artigo 3.º

Objetivos da Política de Segurança da Informação

1 – A segurança da informação tem como principais objetivos garantir os níveis adequados de integridade, autenticidade, disponibilidade e confidencialidade, requeridos para a sua proteção, mitigando assim o impacto de eventuais incidentes que possam comprometer o regular funcionamento do Município de Lagoa.

2 – A integridade consiste na capacidade de prevenir, recuperar e reverter alterações não autorizadas ou acidentais aos dados.

3 – A autenticidade consiste na manutenção da fiabilidade da informação desde o momento da sua produção e ao longo de todo o seu ciclo de vida.

4 – A disponibilidade refere-se à possibilidade de acesso aos dados, quando necessário.

5 – A confidencialidade diz respeito à capacidade de proteger os dados daqueles que não estão autorizados a consultá-los, não impedindo o acesso aos mesmos, em tempo útil, de pessoas autorizadas.

6 – Para o cumprimento destes objetivos, o Município de Lagoa, em conformidade com a legislação e normativos em vigor em matéria de segurança da informação, compromete-se a adotar as melhores práticas nacionais e internacionais.

Artigo 3.º

Âmbito da política de segurança da informação

1 – A política de segurança da informação aplica-se a todas as entidades individuais e coletivas que interagem com a informação sob a responsabilidade do Município de Lagoa, designadamente, aos membros do executivo e respetivos gabinetes de apoio, aos trabalhadores, bem como aos prestadores de serviços externos e entidades que utilizam as instalações e meios do Município de Lagoa, sendo todos eles doravante abreviadamente designados por “utilizadores”.

2 – A presente política aplica-se a toda a informação sob a responsabilidade do Município de Lagoa, independentemente do respetivo suporte de registo, seja ele eletrónico, em papel, audiovisual ou outro.

3 – Além do acesso adequado à informação necessária para o desempenho das suas funções, todos os utilizadores devem ter conhecimento da presente

política, sendo-lhes exigido o respeito pelas respetivas normas de execução e por todos os controlos de segurança implementados.

Artigo 4.º

Conteúdos da política de segurança da informação

1 – A política de segurança da informação do Município de Lagoa consiste na proteção da informação produzida, armazenada, processada ou transmitida no âmbito da atividade municipal, contra a perda de integridade, autenticidade, disponibilidade e confidencialidade.

2 – O Município de Lagoa compromete-se a desenvolver políticas e procedimentos específicos que respeitem as normas internacionais de referência, auditáveis, que definem os requisitos para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), abrangendo, nomeadamente, as áreas previstas nas normas ISO 27001, ISO 27002 e no Regulamento Geral de Proteção de Dados Pessoais, no que respeita a:

a) Recursos Humanos:

i) Assegurar que todos os utilizadores conhecem, entendem e cumprem as responsabilidades na área da segurança da informação em conformidade com as suas funções;

ii) Assegurar que os interesses do Município de Lagoa e dos utilizadores são protegidos como parte do processo de início, mudança ou cessação de funções;

b) Gestão da Informação:

i) Identificar a informação do Município de Lagoa e definir as responsabilidades pela sua proteção;

ii) Definir a política de classificação de segurança, assegurando que a informação receba um nível adequado de proteção de acordo com o seu valor, sensibilidade, criticidade, requisitos legais e riscos a que possa estar sujeita;

iii) Definir a política de uso aceitável que deve conter regras para a utilização dos recursos do Município de Lagoa, ficando o uso destes condicionado à concordância expressa por parte de cada utilizador;

iv) Definir os procedimentos para a gestão dos suportes de armazenamento e salvaguarda da informação;

v) Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação;

c) Gestão de Acessos:

i) Assegurar a gestão e o controlo dos acessos às instalações do Município de Lagoa, ao sistema informático e à informação, responsabilizando os utilizadores pela proteção das suas credenciais de acesso e assegurando a intransferibilidade dos direitos atribuídos através de processos de atribuição de direitos de acesso e privilégio de forma restrita e controlada;

ii) Gerir a divulgação da informação;

d) Segurança Física e Ambiental:

i) Proteger as informações, equipamentos e instalações físicas do Município de Lagoa de acesso não autorizado, dano, interferência, perda, furto ou roubo;

ii) Monitorizar e controlar o ambiente das instalações;

iii) Definir procedimentos que assegurem a salvaguarda dos suportes físicos;

e) Gestão do Sistema Informático:

- i) Garantir a operação e proteção, segura e correta, dos recursos de processamento da informação;
- ii) Registrar e monitorizar eventos e gerar evidências;
- iii) Analisar, controlar, mitigar e eliminar as vulnerabilidades;
- iv) Criar mecanismos que permitam controlar e auditar a conformidade das operações com as políticas de segurança da informação;
- v) Garantir a segurança da informação transmitida dentro da organização e com quaisquer entidades externas;
- vi) Assegurar o uso efetivo e adequado da criptografia para proteger a integridade, autenticidade e integridade da informação;

f) Gestão dos Incidentes de Segurança:

Definir as responsabilidades e os procedimentos a adotar para reagir de forma apropriada perante as fragilidades e incidentes que coloquem em risco a segurança da informação, garantindo o seu registo e prevendo um processo de melhoria contínua e revisão periódica dos processos de gestão de incidentes;

g) Gestão da Continuidade de Serviço:

- i) Garantir que, após a ocorrência de desastres ou falhas de segurança (resultantes, por exemplo, de desastres naturais, acidentes, falhas de equipamentos ou ações intencionais), seja possível manter um nível de funcionamento aceitável até se retornar à situação normal;

- ii) Prever e implementar um plano de continuidade de serviço;

h) Conformidade Legal:

Assegurar o cumprimento dos requisitos de segurança estabelecidos nas obrigações legais, estatutárias, regulamentares e contratuais relativos, entre outros, à Proteção de Dados Pessoais, de modo a:

- i) Identificar e localizar a informação que contém dados pessoais, o seu suporte, propósito, risco e valor;
- ii) Garantir que os procedimentos a estabelecer sejam adequados às obrigações de proteção de dados pessoais decorrentes, nomeadamente, do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, sobre a proteção de dados pessoais e legislação nacional aplicável.

Artigo 5.º

Princípios aplicáveis

As políticas de segurança da informação do Município de Lagoa, quer na sua definição, quer na sua concretização diária, devem orientar-se pelos seguintes princípios:

- a) **Garantia de proteção:** a informação é um recurso crítico para o eficaz desenvolvimento de todas as atividades do Município de Lagoa, sendo assim fundamental garantir a sua adequada proteção, nas vertentes de integridade, autenticidade, disponibilidade e confidencialidade;
- b) **Sujeição à lei:** quer a política de segurança, quer todas as medidas e tarefas executadas na prossecução da mesma, deverão respeitar a legislação aplicável, bem como as normas e regulamentos internos aprovados pelas entidades competentes;

- c) **Necessidade de acesso:** o acesso à informação deve restringir-se, exclusivamente, às pessoas que tenham necessidade de a conhecer para cumprimento das suas funções e tarefas;
- d) **Transparência:** deve assegurar-se a transparência, conjugando o dever de informar com a fixação, de forma clara, das regras e procedimentos a adotar para a segurança da informação sob a responsabilidade do Município de Lagoa;
- e) **Proporcionalidade:** as atividades impostas pela segurança da informação devem ser proporcionais aos riscos a mitigar e limitadas ao necessário, minimizando a entropia no regular funcionamento do Município de Lagoa;
- f) **Obrigatoriedade de cumprimento:** as políticas e procedimentos de segurança definidos devem ser integrados nos processos de trabalho e a execução das tarefas diárias deve ser pautada pelo seu estrito cumprimento;
- g) **Responsabilidades:** as responsabilidades e o papel das entidades intervenientes na segurança da informação devem ser definidas de forma clara e ser alvo de monitorização e auditoria periódicas;
- h) **Informação:** todas as políticas e procedimentos específicos devem ser publicitados e comunicados a todos os utilizadores que deles necessitem para o desempenho das suas funções e tarefas;
- i) **Formação:** deve ser planeado, aprovado e executado um plano de formação e de divulgação que incida sobre o domínio da segurança da informação e sobre as políticas e procedimentos específicos adotados neste âmbito;
- j) **Avaliação do risco:** deve ponderar-se a necessidade de proteção da informação em função da sua relevância e das ameaças que sobre ela incidem. A avaliação do risco deve identificar, controlar e eliminar os diversos

tipos de ameaças a que a informação se encontra sujeita. Os níveis de segurança, custo, medidas, práticas e procedimentos devem ser apropriados e proporcionais ao valor e ao nível de confiança da informação;

- k) **Comunicação, registo e ponto de contacto único:** todos os incidentes de segurança, bem como as fragilidades, têm de ser objeto de comunicação imediata e registo de forma a proporcionar uma resposta célere aos problemas. O processo de registo deve prever a identificação de um ponto único de contacto para onde devem ser canalizados todos os relatos;
- l) **Sanções:** a não observância das disposições de segurança da informação que se encontrem em vigor, será considerada como infração às normas e regulamentos internos e, como tal, será sujeita a medidas corretivas apropriadas de acordo com a legislação e normativos aplicáveis ou que para o efeito venham a ser aprovadas.

Artigo 6.º

Atribuição de responsabilidades

1 – Todos os utilizadores estão obrigados a cumprir e a fazer cumprir a presente política de segurança da informação e têm o dever de zelar pela sua proteção e de proceder à comunicação de qualquer evento que provoque, ou possa provocar, uma quebra de segurança da informação.

2 – O Município de Lagoa é o primeiro responsável pela implementação e controlo do Sistema de Gestão da Segurança da Informação do Município de Lagoa, competindo ao executivo aprovar os seguintes documentos:

- a) Plano de Segurança;
- b) Política de resposta a incidentes;
- c) Política de back-ups e de recuperação;
- d) Normas de gestão de acessos remotos;
- e) Normas de gestão de entidades e acessos;

f) Todos os documentos, normas e outras políticas que devam ser elaboradas na sequência da presente política geral e que sejam indispensáveis à boa execução da mesma.

3 – O Município de Lagoa deve também garantir que sejam atribuídas as autoridades e responsabilidades para as funções da gestão da informação e para o cumprimento das obrigações legais aplicáveis.

4 – O Responsável de Segurança valida e submete à aprovação as propostas relacionadas com a segurança da informação, promove a disponibilização dos meios humanos, financeiros e materiais necessários à gestão da segurança da informação.

5 – Todos os utilizadores devem cumprir e fazer cumprir as políticas, regulamentos e procedimentos relativos à segurança da informação.

6 – Os dirigentes dos serviços ou equiparados devem colaborar com o Responsável de Segurança na definição, implementação e controlo de aplicação das políticas e procedimentos de segurança que vierem a ser definidos para a sua área de competência e são responsáveis por garantir o seu cumprimento por parte dos recursos humanos e materiais sob sua responsabilidade.

7 – Os colaboradores de terceiras entidades que prestam serviço no Município de Lagoa ou que utilizam as suas instalações e meios, bem como os trabalhadores ou empresas contratadas pelo Município, devem cumprir os normativos e procedimentos estipulados na política de segurança da informação do Município de Lagoa.

8 – O Responsável de Segurança é responsável pelas tarefas de implementação, manutenção e operação do sistema, devendo assegurar, designadamente, a gestão de incidentes de segurança, a execução periódica do processo de avaliação dos riscos de segurança, a elaboração dos planos de formação relativos

à segurança da informação e a prestação de apoio às equipas técnicas das especialidades integradas nos processos abrangidos pelo sistema.

9 – O Encarregado da Proteção de Dados é responsável pelo controlo da legislação relativa à proteção de dados pessoais, nomeadamente, nos termos do já referido Regulamento Europeu de Proteção de Dados Pessoais, sendo designado com base nos seus conhecimentos especializados no domínio do Direito e das práticas de proteção de dados, bem como na capacidade para desempenhar as funções exigidas pelo Regulamento.

Artigo 7.º

Implementação

1 – Devem ser implementadas as alterações necessárias às políticas específicas para garantir o cumprimento integral da política definida, exceto quando forem identificadas razões técnicas ou de atividade que inviabilizem a implementação das alterações referidas, devendo tais exceções ser documentadas e acompanhadas por propostas de medidas que possam, entretanto, mitigar os riscos em causa.

2 – De igual modo, sempre que uma ação de renovação tecnológica não conduza ao cumprimento integral da política, deve ser mantida a identificação deste sistema como uma exceção documentada, com a salvaguarda de que nenhuma alteração deve conduzir a uma situação de risco acrescido comparativamente à situação anterior.

Artigo 8.º

Entrada em vigor e revisão

1 – A presente Política Geral de Segurança da Informação entra em vigor no dia seguinte ao da sua publicação e será revista sempre que seja considerado necessário.

2 – A entrada e vigor do presente regulamento revoga o Regulamento Interno de Sistemas de Informação do Município de Lagoa, aprovado em 2020.